

Osamu Kawamura et al

82478-8100

日 本 国 特 許 庁
JAPAN PATENT OFFICE

JDW Price

949-253-4820

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年 8月27日

出 願 番 号

Application Number:

特願2002-247693

[ST.10/C]:

[JP2002-247693]

出 願 人

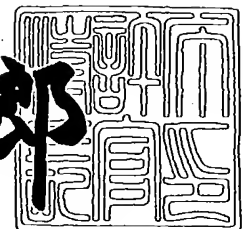
Applicant(s):

松下電器産業株式会社

2003年 5月 9日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3033611

【書類名】 特許願

【整理番号】 2022540038

【提出日】 平成14年 8月27日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 1/00
H04L 9/00

【発明者】

【住所又は居所】 大阪府門真市大字門真1 0 0 6 番地 松下電器産業株式会社内

【氏名】 河村 領

【発明者】

【住所又は居所】 大阪府門真市大字門真1 0 0 6 番地 松下電器産業株式会社内

【氏名】 尾坂 匡隆

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100090446

【弁理士】

【氏名又は名称】 中島 司朗

【手数料の表示】

【予納台帳番号】 014823

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9003742

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 並列ストリーム暗復号装置及びその方法並びに並列ストリーム暗復号プログラム

【特許請求の範囲】

【請求項 1】 ストリームデータを暗号化又は復号化する複数の鍵にそれぞれ対応する複数の経路と、

入力される複数のストリームデータを、対応する経路に出力する入力ストリーム処理手段と、

出力されたストリームデータを対応する鍵で暗号化又は復号化する暗復号演算手段とを備えることを特徴とする並列ストリーム暗復号装置。

【請求項 2】 前記入力ストリーム処理手段は、クロスバスイッチを有し、ストリームデータの入力線とストリームデータを暗号化又は復号化する鍵に対応する経路に接続される出力線との接点のスイッチをオンに設定することにより、対応する経路にストリームデータを出力することを特徴とする請求項 1 記載の並列ストリーム暗復号装置。

【請求項 3】 前記暗復号演算手段で暗号化又は復号化された複数のストリームデータの入力を受け、複数の出力インターフェースに各暗号化又は復号化されたストリームデータをそれぞれ出力する出力ストリーム処理手段を更に備えることを特徴とする請求項 1 記載の並列ストリーム暗復号装置。

【請求項 4】 前記出力ストリーム処理手段は、クロスバスイッチを有し、前記出力ストリーム処理手段から出力される複数の暗号化又は復号化されたストリームデータの出力先の出力インターフェースを前記経路に応じてクロスバスイッチをオンオフ制御して切り換える制御手段と、

複数の経路へ出力されたストリームデータと対応する鍵とを前記暗復号演算手段に経路毎に入力し、入力したストリームデータの経路情報を前記制御手段に通知する入力通知手段を更に備えることを特徴とする請求項 3 記載の並列ストリーム暗復号装置。

【請求項 5】 前記暗復号演算手段を複数備え、

前記複数の経路へ出力されるストリームデータと対応する鍵とを各暗復号演算

手段に並列入力し、各暗復号演算手段に入力したストリームデータの経路情報を通知する入力通知手段と、

前記経路情報に従い、前記出力ストリーム処理手段から出力される複数の暗号化又は復号化されたストリームデータの出力先の出力インターフェースを選択制御する制御手段とを更に備えることを特徴とする請求項3記載の並列ストリーム暗復号装置。

【請求項6】 前記暗復号演算手段から出力された暗号化又は復号化されたストリームデータを再度前記入力ストリーム処理手段に入力する経路を更に備え、

前記暗復号演算手段は、暗号化又は復号化されたストリームデータを異なる鍵で暗号化又は復号化することを特徴とする請求項1記載の並列ストリーム暗復号装置。

【請求項7】 前記入力ストリーム処理手段は、入力される複数のストリームデータをマルチプレクス処理して1つのストリームデータを生成することを特徴とする請求項1記載の並列ストリーム暗復号装置。

【請求項8】 前記入力ストリーム処理手段は、入力される1つのストリームデータをデマルチプレクス処理して複数のストリームデータを生成することを特徴とする請求項1記載の並列ストリーム暗復号装置。

【請求項9】 前記入力ストリーム処理手段は、入力される1つのストリームデータを2つの経路に出力し、

1つの経路は、前記暗復号演算手段に、別の経路は、直接前記出力ストリーム処理手段にそれぞれ接続されていることを特徴とする請求項3記載の並列ストリーム暗復号装置。

【請求項10】 ストリームデータを暗号化又は復号化する複数の鍵にそれぞれ対応する複数の経路を備える並列ストリーム暗復号装置における並列ストリーム暗復号方法であって、

入力される複数のストリームデータを、対応する経路に出力する入力ストリーム処理ステップと、

出力されたストリームデータを対応する鍵で暗号化又は復号化する暗復号演算

ステップとを有することを特徴とする並列ストリーム暗復号方法。

【請求項 1 1】 請求項 1 0 記載の並列ストリーム暗復号方法をコンピュータに実行させるプログラム。

【請求項 1 2】 請求項 1 記載の並列ストリーム暗復号装置を組み込んだ T V 受信装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、受信した番組を記録する記録装置を有する T V 受信装置に組み込まれる複数のストリームデータを並列に暗号化、復号化する並列ストリーム暗復号装置に関する。

【0 0 0 2】

【従来の技術】

最近、T V 受信装置は、放送局から放送される放送番組を受信して放映するだけでなく、例えば、インターネットのブロードバンド放送の番組を通信回線を経由して受信して放映したり、受信した番組を例えば H D D に蓄積し、後で視聴できるようにと種々の形態で使用されている。また、市販の D V D (デジタル多目的ディスク) 等のコンテンツの再生も T V 受信装置を利用して行われている。

【0 0 0 3】

これらの放送番組等のコンテンツは、著作権保護等を目的として暗号化されて放送されているので、復号化する必要がある。また、一旦復号化したコンテンツを記録媒体に記録するとき、再度暗号化を施す場合がある。

図 1 6 は、T V 受信装置に組み込まれた従来の並列ストリーム暗復号装置の構成図である。

【0 0 0 4】

この並列ストリーム暗復号装置は、入力インターフェース 1 6 0 1 ~ 1 6 0 5 と、ストリーム解析部 1 6 1 0 と、制御部 1 6 1 1 と、ストリーム処理部 1 6 2 1 と、鍵 1 6 3 1 ~ 1 6 3 4 と、セクタ 1 6 3 5 と、転送調停部 1 6 5 1 と、暗復号演算部 1 6 6 1 と、セクタ 1 6 7 1 と、出力インターフェース 1 6 8 1

～1685とを備えている。

【0005】

例えば、視聴番組のストリームデータを入力インターフェース1601から、録画番組のストリームデータを入力インターフェース1602からそれぞれ入力し、これらの暗号化されたストリームデータを暗復号演算部1661で復号して、復号したストリームデータを視聴番組は出力インターフェースは1681から、録画番組は出力インターフェース1682からそれぞれ出力する場合について説明する。

【0006】

視聴番組の復号のための復号鍵を鍵1631に設定し、録画番組の復号のための復号鍵を鍵1632に設定する。

ストリーム解析部1610は、入力インターフェース1601、1602からそれぞれ入力されるストリームデータの packets からヘッダ情報を抽出し、当該 packets の P I D が視聴番組又は録画番組の P I D と一致するか否かを制御部1611に通知する。制御部1611は、一致するときには、ストリーム処理部1621に当該 packets を出力するよう入力インターフェース1601、1602に指示し、一致しないときには、廃棄するよう指示する。また、制御部1611は、ストリーム処理部1621に入力インターフェース1601、1602のいずれの packets の処理であるかを通知する。

【0007】

入力ストリーム処理部1621は、入力された packets のフォーマットを変換し、暗復号演算部1661に出力する。この際、転送調停部1651に入力インターフェース1601、1602の何れからのデータであるかを通知する。

転送調停部1651は、ストリーム処理部1621から暗復号演算部1661に出力したデータが入力インターフェース1601のものであるときには、復号鍵1631を暗復号演算部1661に通知するようセレクタ1635に指示する。出力したデータが入力インターフェース1602のものであるときには、復号鍵1632を暗復号演算部1661に通知するようセレクタ1635に指示する。

【 0 0 0 8 】

暗復号演算部 1 6 6 1 は、ストリーム処理部 1 6 2 1 から入力されるデータをセクタ 1 6 3 5 から通知される復号鍵 1 6 3 1 又は、復号鍵 1 6 3 2 で復号化する。復号化が完了すると復号化したデータをセクタ 1 6 7 1 に出力するとともに、転送調停部 1 6 5 1 に通知する。

転送調停部 1 6 5 1 は、復号化されたデータを出力インターフェース 1 6 8 1 又は出力インターフェース 1 6 8 2 のいずれに出力するかをセクタ 1 6 7 1 に指示する。セクタ 1 6 7 1 は、暗復号演算部 1 6 6 1 から入力された復号化されたデータを転送調停部 1 6 5 1 から指示された出力インターフェース 1 6 8 1 、 1 6 8 2 にそれぞれ出力する。

【 0 0 0 9 】

【発明が解決しようとする課題】

ところで、上記従来の並列ストリーム暗復号装置では、暗復号演算部 1 6 6 1 でデータの復号化の際に、復号鍵 1 6 3 1、 1 6 3 2 をセクタ 1 6 3 5 でストリーム処理部 1 6 2 1 からのデータ入力毎に選択しなければならない。

このセクタ 1 6 3 5 での復号鍵 1 6 3 1、 1 6 3 2 の選択のための制御手順は複雑である。

【 0 0 1 0 】

本発明は、上記課題に鑑みなされたものであり、鍵選択の煩雑さを回避して並列入力されるストリームデータの暗復号のスループットの向上された並列ストリーム暗復号装置及びその方法を提供することを目的とする。

【 0 0 1 1 】

【課題を解決するための手段】

上記課題を解決するため、本発明はストリームデータを暗号化又は復号化する複数の鍵にそれぞれ対応する複数の経路と、入力される複数のストリームデータを、対応する経路に出力する入力ストリーム処理手段と、出力されたストリームデータを対応する鍵で暗号化又は復号化する暗復号演算手段とを備えることとしている。

【 0 0 1 2 】

【発明の実施の形態】

以下、本発明に係る並列ストリーム暗復号装置の実施の形態について、図面を用いて説明する。

(実施の形態 1)

図 1 は、本発明に係る並列ストリーム暗復号装置の実施の形態 1 の構成図である。

【0013】

この並列ストリーム暗復号装置は、入力インターフェース 101～105 と、ストリーム解析部 110 と、ストリーム制御部 111 と、入力ストリーム処理部 121 と、調停部 151 と、暗復号演算部 161 と、出力ストリーム処理部 171 と、出力インターフェース 181～185 とを備え、入力ストリーム処理部 121 と調停部 151 間には、鍵 131～134 にそれぞれ対応付けられた経路 141～144 が設けられている。

【0014】

なお、この並列ストリーム暗復号装置は TV 受信装置に組み込まれている。

入力インターフェース 101～105 は、アンテナ、外部装置、CATV 回線、公衆回線網とそれぞれ接続され、入力されるストリームデータをストリーム解析部 110 に通知し、ストリーム制御部 111 からの出力指示に従い、入力ストリーム処理部 121 にストリームデータを出力する。

【0015】

例えば、入力インターフェース 101 は、アンテナに接続され、TV 放送の番組のストリームデータの入力を受け、番組視聴用に出力する。入力インターフェース 102 は、同様に TV 放送の番組のストリームデータの入力を受け、番組録画用に出力する。入力インターフェース 103 は、DVD ドライブ装置に接続され、DVD に記録されたストリームデータの入力を受け、出力する。入力インターフェース 104 は、CATV 回線に接続され、入力されるストリームデータを出力する。入力インターフェース 105 は、公衆回線網に接続され、インターネット放送によるストリームデータの入力を受け、出力する。

【0016】

なお、入力インターフェース 1 0 1 ~ 1 0 5 の接続先は、適宜変更されて実施される。

TV受信装置において、視聴者が視聴したい番組と録画したい番組とをチャンネルを選択して指定したとき、TV受信装置の制御部（図示せず）は、入力インターフェース 1 0 1 に視聴番組のトランスポートストリーム（TS）を、入力インターフェース 1 0 2 に録画番組の TS を入力するよう、アンテナ等を設定するとともに、ストリーム解析部 1 1 0 に視聴番組と録画番組との TS パケットの PID（パケット識別子）を通知し、鍵 1 3 1 に暗号化された視聴番組を復号する復号鍵を設定し、鍵 1 3 2 に暗号化された録画番組を復号する復号鍵を設定する。更に、ストリーム制御部 1 1 1 に入力インターフェース 1 0 1 からのデータを経路 1 4 1 に、入力インターフェース 1 0 2 からのデータを経路 1 4 2 に出力するよう指示する。また、ストリーム制御部 1 1 1 に、出力ストリーム処理部 1 7 1 において経路 1 4 1 を経由した復号化されたデータを出力インターフェース 1 8 1 に、経路 1 4 2 を経由した復号化されたデータを出力インターフェース 1 8 2 にそれぞれ出力するように指示する。

【0017】

入力インターフェース 1 0 1 は、視聴番組の TS の入力を受けると、TS パケットを抽出し、そのうちのヘッダ情報をストリーム解析部 1 1 0 に通知する。

ストリーム制御部 1 1 1 から出力指示を受けると抽出した TS パケットを入力ストリーム処理部 1 2 1 に出力する。また、廃棄指示を受けると抽出した TS パケットを廃棄する。

【0018】

入力インターフェース 1 0 2 は、録画番組の TS の入力を受けると、TS パケットを抽出し、ヘッダ情報をストリーム解析部 1 1 0 に通知する。

ストリーム制御部 1 1 1 から出力指示を受けると抽出した TS パケットを入力ストリーム処理部 1 2 1 に出力する。また、廃棄指示を受けると抽出した TS パケットを廃棄する。

【0019】

ストリーム解析部 1 1 0 は、TV受信装置の制御部から入力インターフェース

101と入力インターフェース102とにそれぞれ入力されるTSから抽出すべきTSパケットのPIDの通知を受ける。

ストリーム解析部110は、入力インターフェース101と入力インターフェース102とからそれぞれTSパケットのヘッダ情報の通知を受けると、ヘッダ情報に含まれるPIDがTV受信装置の制御部から通知されているそれぞれのPIDと一致するか否かを判定し、その結果をストリーム制御部111に通知する。

【0020】

ストリーム制御部111は、TV受信装置の制御部から入力インターフェース101からのデータを経路141に、入力インターフェース102からのデータを経路142に出力するよう指示され、出力ストリーム処理部216に経路141を経由した復号化されたデータを出力インターフェース181に、経路142を経由した復号化されたデータを出力インターフェース182にそれぞれ出力するように指示される。

【0021】

また、ストリーム制御部111は、ストリーム解析部110からTSパケットのヘッダ情報の解析結果、即ち、所望のPIDを有するTSパケットか否かの通知を受けると、PIDが一致するときには、入力インターフェース101、入力インターフェース102に入力ストリーム処理部121に当該TSパケットを出力するようそれぞれ指示する。またPIDが一致しないときには、当該TSパケットを廃棄するようそれぞれ指示する。

【0022】

ストリーム制御部111は、前述したTV受信装置の制御部からの経路141、142への出力指示に応じて入力ストリーム処理部121が有するクロスバスイッチのオン、オフを設定する。

図2は、入力ストリーム処理部121のクロスバスイッチを示している。クロスバスイッチ201の入力線202と出力線203との接点の印で示すスイッチ204、205をオンにする。○印はオフを示している。これによって、入力インターフェース101からのデータは経路141に、入力インターフェース1

02からのデータは経路142にそれぞれ出力されるようになる。

【0023】

ストリーム制御部111は、調停部151から暗復号演算部161に出力したデータが経路141又は経路142のいずれの経路からのデータであるかの通知を受ける。通知された経路141又は経路142に応じて出力ストリーム処理部171が有するクロスバスイッチのオン、オフを設定してデータの出力先の出力インターフェース181～185を切り換える。

【0024】

入力ストリーム処理部121は、入力インターフェース101、102からそれぞれTSパケットの入力を受けると、伝送用のストリーム形式からコンテンツデータとして利用可能な形式に変換する。例えば、PES（パケッタイズド・エレメンタリー・ストリーム）パケットにフォーマットを変換する。変換したPESパケットは、暗号化データを復号するため設定された復号鍵131、132に対応する経路に出力する。

【0025】

図2に示したように、入力ストリーム処理部121が有するクロスバスイッチ201のスイッチ204、205がオンにされている。これによって、視聴番組のPESパケットを復号鍵131に対応する経路141に出力し、録画番組のPESパケットを復号鍵132に対応する経路142に出力する。

鍵131～134は、レジスタで構成され、TV受信装置の制御部により、視聴者のチャンネル選択に応じた番組の復号鍵がそれぞれ設定される。

【0026】

調停部151は、経路141と経路142とからそれぞれ、視聴番組のPESパケットと録画番組のPESパケットの入力を受ける。視聴番組のPESパケットの入力を受けたときは、視聴番組の復号鍵131とともに暗復号演算部161に出力する。同様に、録画番組のPESパケットの入力を受けたときは、録画番組の復号鍵132とともに暗復号演算部161に出力する。

【0027】

なお、本実施の形態では、ストリームの区切り（パケット）を復号単位として

いるので、PES パケット単位で暗復号演算部 161 に出力するようにしたけれども、ブロック暗復号の場合には、暗復号演算単位で出力する。例えば、DES 暗号のときには、8 バイト単位でデータを出力する。

また、調停部 151 は、暗復号演算部 161 にデータを出力したとき、いずれの経路から入力されたデータであるのかをストリーム制御部 111 に通知する。

【0028】

また、経路 141 と経路 142 とから同時に PES パケットの入力を受けたときには、例えば、経路 141 のデータを優先して暗復号演算部 161 に出力する。これは、視聴番組の方が録画番組よりもリアルタイム性が優先されることによる。全ての経路 141 ～144 からデータが入力されているときには、例えば、もっとも長い間出力されていない経路のデータを最優先して出力するようにしてもよい。なお、どのようなルールで暗復号演算部 161 にデータを出力するかは、予め TV 受信装置の制御部により設定されるものとする。

【0029】

暗復号演算部 161 は、入力されるデータに暗号化又は復号化の演算を行い暗号化データ又は復号化データを出力ストリーム処理部 171 に出力する。

暗復号演算部 161 は、調停部 151 から復号鍵 131 と PES パケットとの入力又は復号鍵 132 と PES パケットとの入力を受けると、それぞれの復号鍵 131 又は復号鍵 132 を用いて PES パケットのデータを復号化する。復号化した PES パケットのデータを出力ストリーム処理部 171 に出力する。

【0030】

出力ストリーム処理部 171 は、クロスバスイッチを有し、暗復号演算部 161 で暗号化又は復号化されたデータの入力を受け、フラグ情報等の制御情報を変換して所定の出力インターフェースに出力する。

図 3、図 4 は、出力ストリーム処理部 171 でのクロスバスイッチの状態を説明する図である。

【0031】

図 3 では、クロスバスイッチ 301 の入力線 302 と出力線 303 との接点 304 がスイッチオンの状態となっている。これは、調停部 151 からストリーム

制御部111に経路141からのPESパケットのデータ出力をしたことが通知され、ストリーム制御部111が、接点304のスイッチをオンにしたことによる。これによって、入力インターフェース101から入力されたTSデータは復号化されて出力インターフェース181から出力される。

【0032】

出力ストリーム処理部171は、入力されたデータが暗復号演算部161で復号されているので、例えば、PES中の「スクランブルがかかっている」というフラグを「スクランブルがかかっていない」というフラグに変更する。また、ストリーム中に番組情報一覧が含まれるときに、入力インターフェース部101でPIDが一致しないとして廃棄されたパケットデータに関する情報を削除する。

【0033】

図4は、調停部151からストリーム制御部111に経路142からのPESパケットのデータ出力をしたことが通知され、ストリーム制御部111がクロスバススイッチ301の接点304のスイッチをオフにし、接点401のスイッチをオンにした状態を示している。

暗復号演算部101から入力された復号化されたPESデータは、入力線302から出力線303を介して出力インターフェース182に出力される。この際、PESデータのフラグが「スクランブルがかかっていない」に変更されるとともに、番組情報中の削除された番組についての番組情報の変更処理がなされる。

【0034】

出力インターフェース181は、TV受信装置の表示部（図示せず）に接続され、出力ストリーム処理部171から入力された復号化されたデータを表示部に出力し、TV番組を放映させる。

出力インターフェース182は、TV受信装置が内蔵するHDDで構成される録画部（図示せず）に接続され、出力ストリーム処理部171から入力された復号化されたデータを録画部に出力し、TV番組を録画させる。

【0035】

次に、本実施の形態の動作を図5に示すフローチャートを用いて説明する。

TV受信装置の制御部は、ユーザからの視聴番組と録画番組とのチャンネル指定

に応じて、入力インターフェース101～105、出力インターフェース181～185を選択し、入力インターフェース101～105での抽出すべきTSパケットのPIDをストリーム解析部110に通知し、鍵131から134に視聴番組と録画番組との復号鍵をそれぞれ設定する。また、ストリーム制御部111に鍵131～134のいずれに視聴番組と録画番組との復号鍵を設定したかを通知する(S502)。

【0036】

選択された入力インターフェース101、102は、それぞれTSデータの入力を待ち(S504)、TSパケットを抽出し、ヘッダ情報をストリーム解析部110に通知する(S506)。

ストリーム解析部110は、入力インターフェース101、102にそれぞれ設定されたPIDと一致するTSパケットが入力されたか否かを判定する(S508)。ストリーム解析部110は、判定結果をストリーム制御部111に通知する。

【0037】

ストリーム制御部111は、判定結果が一致しないときは、入力インターフェース部101、102に一致しないTSパケットの廃棄を指示し、S504に戻る。一致するときには、入力インターフェース部101、102に入力ストリーム処理部121にパケットデータの出力指示をする(S510)。

ストリーム制御部111は、TV受信装置の制御部から通知された復号鍵の設定に応じて、入力ストリーム処理部121から調停部151間の経路141～144のいずれの経路を入力インターフェース101、102からのデータに使用するかを定めるため、入力ストリーム処理部121のクロスバスイッチ201のオン、オフを設定する(S512)。

【0038】

入力ストリーム処理部121は、入力インターフェース101、102からそれぞれ入力されたパケットデータのフォーマットを変換し、例えばPES形式に変換し(S514)、決定された経路141、142をそれぞれ介して調停部151に出力する(S516)。

調停部 1 5 1 は、経路 1 4 1、1 4 2 を介してデータが入力されると経路 1 4 1、1 4 2 にそれぞれ対応して設定された復号鍵と当該データとを経路 1 4 1、1 4 2 の優先順に暗復号演算部 1 6 1 に出力するとともに、ストリーム制御部 1 1 1 に入力経路 1 4 1、1 4 2 の別を通知する（S 5 1 8）。

【0 0 3 9】

ストリーム制御部 1 1 1 は、暗復号演算部 1 6 1 に入力されるデータの経路 1 4 1、1 4 2 に応じて出力インターフェース 1 8 1 ～ 1 8 5 を決定するため、クロスバスイッチ 3 0 1 のオン、オフを設定する（S 5 2 0）。

暗復号演算部 1 6 1 は、調停部 1 5 1 から入力された復号鍵を用いて、入力された暗号化データを復号演算処理して、復号化データを出力ストリーム処理部 1 7 1 に出力する（S 5 2 2）。

【0 0 4 0】

出力ストリーム処理部 1 7 1 は、復号化データの制御情報等を変更して、決定された出力インターフェース 1 8 1、1 8 2 にそれぞれ出力する（S 5 2 4）。

ストリーム制御部 1 1 1 は、調停部 1 5 1 から入力経路 1 4 1、1 4 2 の通知があるか否かを判定し（S 5 2 6）、あるときは S 5 2 0 に戻り、なければ、終了指示が TV 受信装置の制御部から有るか否かを判定し（S 5 2 8）、なければ S 5 0 4 に戻り、あるときには処理を終了する。

（実施の形態 2）

図 6 は、本発明に係る並列ストリーム暗復号装置の実施の形態 2 の構成図である。

【0 0 4 1】

この並列ストリーム暗復号装置は、上記実施の形態 1 の並列ストリーム暗復号装置の暗復号演算部 1 6 1 に替えて、第 1 暗復号演算部 6 0 1 と第 2 暗復号演算部 6 0 2 とを備え、これに応じて調停部 1 5 1 に替えて、第 1 調停部 6 0 3 と第 2 調停部 6 0 4 とを備えている。また、第 1 暗復号演算部 6 0 1 と出力ストリーム処理部 6 0 7 との間には経路 6 0 5 が、第 2 暗復号演算部 6 0 2 と出力ストリーム処理部 6 0 7 との間には経路 6 0 6 がそれぞれ設けられている。また、第 1 調停部 6 0 3 又は第 2 調停部 6 0 4 のいずれかに、鍵 1 3 1 ～ 1 3 4 にそれぞれ

対応する経路141～144が接続される。この経路141～144と第1調停部603又は第2調停部604との接続は、TV受信装置の制御部（図示せず）により、鍵131～134の設定とともになされる。なお、本実施の形態では、経路141、142と第1調停部603とが、経路143、144と第2調停部604とが予め接続されているものとして説明する。

【0042】

他の構成は、上記実施の形態1とほぼ同様であるので、説明を省略し、本実施の形態固有の構成について説明する。

入力インターフェース101から入力ストリーム処理部121には、上記実施の形態1と同様、放送番組のTSパケットが入力される。入力インターフェース103から入力ストリーム処理部121には、DVDドライブ装置（図示せず）から入力されたプログラムストリーム（PS）パケットが入力される。

【0043】

図7に示すように、入力ストリーム処理部121のクロスバスイッチ701の接点702、703がストリーム制御部111によってオン状態にされている。

入力ストリーム処理部121は、入力インターフェース101から入力されたTSパケットをPESに変換し、経路141に出力する。入力インターフェース103から入力されたPSパケットは無変換のまま、経路143に出力する。

【0044】

第1調停部603は、経路141からPES形式のデータの入力を受けると、復号鍵131とともに第1暗復号演算部601に出力する。同様に第2調停部604は、経路143からPSパケットのデータの入力を受けると、復号鍵133とともに第2暗復号演算部602に出力する。

第1暗復号演算部601は、入力されたデータを復号鍵131で復号し、経路605を介して出力ストリーム処理部607に出力する。

【0045】

第2暗復号演算部602は、入力されたデータを復号鍵133で復号し、経路606を介して出力ストリーム処理部607に出力する。

図8は、出力ストリーム処理部607が有するクロスバスイッチ801の設定

状態を示している。第1暗復号演算部601から出力される復号化されたデータの経路605に接続された入力線と出力インターフェース181に接続される出力線との接点802のスイッチがストリーム制御部111によってオンにされている。また、第2暗復号演算部602から出力される復号化されたデータの経路606に接続された入力線と出力インターフェース183に接続される出力線との接点803のスイッチがストリーム制御部111によってオンにされている。これによって、第1暗復号演算部601で復号化された放送番組のPES形式のデータは、出力ストリーム処理部607で「スクランブルがかかっていない」にフラグ変換され、出力インターフェース181に出力される。出力インターフェース181は、このデータの入力を受け、図示しないTV受信装置の表示部に放送番組を出力する。

【0046】

また、第2暗復号演算部602で復号化されたDVDに記録されたPSのデータは、出力ストリーム処理部607で「暗号化されていない」にフラグ変更され、出力インターフェース183に出力される。出力インターフェース183は、このデータの入力を受け、図示しない外部のビデオ記録装置にこのPSのデータを出力する。

【0047】

本実施の形態では、入力ストリーム処理部121に入力される入力インターフェース101、103からの並列ストリームを第1暗復号演算部601と第2暗復号演算部602とで並列に復号演算するようにしている。2個の暗復号演算部601、602とを設けることで、入力された2つのストリームデータの処理を時分割処理することなく並列処理が可能となる。更に、出力ストリーム処理部607のクロスバススイッチ801のオン、オフの切換操作もストリームデータの入力される最初に1度設定しておくだけで、実施の形態1のように、調停部151からの経路通知毎に切換える必要がなくなる。

【0048】

また、本実施の形態では、放送番組のTSとDVDに記録されたPSとの異なる暗号アルゴリズムで暗号化されたストリームデータについて、それぞれ復号処

理をするようにしている。このような場合、1つの暗復号演算部を用いて時分割で処理するより、2個の暗復号演算部を用いる方が切り替え操作を必要とせず、処理効率が特に向上する。

【0049】

次に、本実施の形態の動作を図9に示すフローチャートを用いて説明する。なお、図中のS512までは、上記実施の形態1と同様であるのでその説明を省略する。

S902において、入力ストリーム処理部121は、入力インターフェース101から入力されたTSパケットをPE S形式のデータに変換し、入力インターフェース103から入力されたPSパケットは無変換のPS形式で、設定された第1調停部603又は第2調停部604にそれぞれ出力する(S904)。

【0050】

第1調停部603と第2調停部604とは、入力されたデータと復号鍵131又は復号鍵133とを第1暗復号演算部601と第2暗復号演算部602とにそれぞれ出力する。併せて、ストリーム制御部111に第1暗復号演算部601又は第2暗復号演算部602にデータを出力したことを通知する(S906)。

ストリーム制御部111は、出力ストリーム制御部607の有するクロスバスイッチ801のスイッチのオン、オフを設定する(S908)。

【0051】

第1暗復号演算部601と第2暗復号演算部602とは、それぞれ、入力された復号鍵131、133を用いて入力されたデータを復号演算処理して復号化したデータを出力ストリーム処理部607に出力する(S910)。

出力ストリーム処理部607は、入力された復号化された各データのフラグ等を変更して設定された出力インターフェース181、183に出力する(S912)。

【0052】

ストリーム制御部111は、TV受信装置の制御部から終了指示があるか否かを判定し(S914)、なければS504に戻り、あれば処理を終了する。

なお、本実施の形態では、第1暗復号演算部601と第2暗復号演算部602

とを設けたけれども、入力ストリーム処理部121からデータが出力される経路141～144の数と同数又はそれ以上の数の暗復号演算部を設けるようにしてもよい。即ち、鍵131～134と同数の暗復号演算部を設けて、暗号化、復号化の並列処理をするようにしてもよいし、又異なる暗復号アルゴリズムの暗復号演算部を予め設けるようにしてもよい。この場合、調停部を暗復号演算部に対応して設けなければならない。

【0053】

次に、図10は、上記実施の形態1又は2の変形例である入力ストリーム処理部121のクロスバスイッチの設定状態を示している。

入力インターフェース102から入力される録画用の番組のTSストリームをTV受信装置に内蔵するHDDで蓄積するとともに、外部のビデオ録画装置でも記録するように、出力インターフェース182、183に出力するため、入力ストリーム処理部121は、PES形式に変換されたデータを経路142、143とに出力する。

【0054】

ストリーム制御部111は、クロスバスイッチ1001の接点1002、1003とをオンに設定している。

また、別の変形例として、入力インターフェース102から2チャンネルの番組のTSストリームが入力されている場合、ストリーム解析部110で各チャンネルに対応するPIDをストリーム制御部111に通知する。ストリーム制御部111は、接点1002、1003とを2個のPIDに応じてオン、オフを制御する。これによって、経路142には1のチャンネルの番組のPESパケットを、経路143には他のチャンネルの番組のPESパケットをそれぞれ出力することになる。入力ストリーム処理部121は、デマルチプレクス処理をすることになる。

【0055】

図11は、更に他の変形例である入力ストリーム処理部121のクロスバスイッチの設定状態を示している。

クロスバスイッチ1101の接点1102、1103がオンに設定されている。

入力インターフェース 1 0 1 には、有る番組に一定時間毎にある CM の挿入された TS ストリームが入力されている。入力インターフェース 1 0 2 には、別の番組に一定時間毎に別の CM の挿入された TS ストリームが入力されている。

【 0 0 5 6 】

ストリーム制御部 1 1 1 は、入力インターフェース 1 0 1 にある番組の TS パケットの出力指示とある CM の TS パケットの廃棄指示とをし、入力インターフェース 1 0 2 に別の番組の TS パケットの廃棄指示と別の CM の TS パケットの出力指示とをする。

入力ストリーム処理部 1 2 1 では、2 つの TS ストリームを 1 つの TS ストリームにするマルチプレクス処理が行われる。即ち、経路 1 4 2 には、ある番組の TS パケットと別の CM の TS パケットが 1 つの TS ストリームとして出力される。

【 0 0 5 7 】

なお、図 1 0、図 1 1 では、入力ストリーム処理部 1 2 1 でのデマルチプレクス処理と、マルチプレクス処理とを説明したけれども、出力ストリーム処理部 1 7 1 等でデマルチプレクス処理とマルチプレクス処理とが行われるようにしてもよいのは勿論である。

(実施の形態 3)

図 1 2 は、本発明に係る並列ストリーム暗復号装置の実施の形態 3 の構成図である。

【 0 0 5 8 】

この並列ストリーム暗復号装置は、上述した実施の形態 1 のそれと、入力ストリーム処理部 1 2 0 1 と調停部 1 5 1 との間の経路 1 2 1 1 ~ 1 2 1 4 に分岐経路 1 2 2 1 ~ 1 2 2 4 をそれぞれ設け、分岐経路 1 2 2 1 ~ 1 2 2 4 を出力ストリーム処理部 1 2 0 3 にそれぞれ接続していることと、暗復号演算部 1 6 1 と出力ストリーム処理部 1 2 0 3 との間の経路 1 2 3 1 に分岐経路 1 2 4 1 を設け、分岐経路 1 2 4 1 を入力インターフェース 1 0 5 に接続していることとが異なるだけである。

【 0 0 5 9 】

以下、本実施の形態固有の構成についてのみ説明する。

本実施の形態では、暗号化された番組のTSの入力を入力インターフェース101が受け、この番組を視聴するとともに、暗号化された状態の番組を内蔵のHDDに記録し、更に、一旦復号化した番組を別の暗号鍵で暗号化して外部のビデオ記録装置に記録する。

【0060】

出力インターフェース181は、TV受信装置の表示部に復号化されたデータを出し、出力インターフェース182は、HDDに暗号化されたままのデータを出し、出力インターフェース183は、再暗号化したデータを外部のビデオ記録装置に出力する。

図13は、入力ストリーム処理部1201のクロスバスイッチの設定状態を示している。クロスバスイッチ1301の接点1302、1303がオンに設定されている。

【0061】

入力インターフェース101は、番組のTS入力を受け、ストリーム制御部111の出力指示により、入力ストリーム処理部1201にTSパケットを出力する。入力ストリーム処理部1201は、入力されたTSパケットをPES形式のパケットに変換する。PES形式のパケットは、クロスバスイッチ1301を経由して、経路1211、1221に出力される。経路1221に出力されたデータは、出力ストリーム処理部1203に直接入力される。経路1211に出力されたPES形式のパケットは、調停部151に出力される。

【0062】

調停部151は、入力されたPES形式のパケットと復号鍵131とを暗復号演算部161に出力し、ストリーム制御部111に経路1211から入力されたデータを暗復号演算部161に出力したことを通知する。

暗復号演算部161は、入力されたデータを復号鍵131で復号化し、復号したデータを経路1231、1241に出力する。経路1231に出力された復号化されたデータは、出力ストリーム処理部1203に入力される。

【0063】

経路 1 2 4 1 に出力された復号化されたデータは、入力インターフェース 1 0 5 に入力される。ストリーム制御部 1 1 1 は、入力インターフェース 1 0 5 に入力されたデータが経路 1 2 1 1 を経由したデータであるとき、入力ストリーム処理部 1 2 0 1 への出力指示をする。

なお、経路 1 2 1 3 を経由したデータが経路 1 2 4 1 から入力インターフェース 1 0 5 に入力されたときには、ストリーム制御部 1 1 1 は、そのデータの廃棄を指示する。

入力ストリーム処理部 1 2 0 1 は、入力インターフェース 1 0 5 から入力された復号化されたデータを無変換でクロスバススイッチ 1 3 0 1 を経由して、経路 1 2 1 3、1 2 2 3 に出力する。ここで、無変換としているのは、このデータが既に P E S 形式の packets に変換されているからである。

【 0 0 6 4 】

経路 1 2 2 3 に出力された復号化されたデータは、出力ストリーム処理部 1 2 0 3 に入力される。

経路 1 2 1 3 に出力されたデータは、調停部 1 5 1 に入力される。調停部 1 5 1 は、このデータと暗号鍵 1 3 3 とを暗復号演算部 1 6 1 に出力するとともに、ストリーム制御部 1 1 1 に経路 1 2 1 3 から入力されたデータを暗復号演算部 1 6 1 に出力したことを通知する。

【 0 0 6 5 】

暗復号演算部 1 6 1 は、暗号鍵 1 3 3 を用いてデータを暗号化し、暗号化したデータを経路 1 2 3 1、1 2 4 1 に出力する。経路 1 2 3 1 に出力された暗号化されたデータは、出力ストリーム処理部 1 2 0 3 に入力され、経路 1 2 4 1 に出力された暗号化されたデータは再び入力インターフェース 1 0 5 に入力される。なお、この暗号化されたデータは、上述のように入力インターフェース 1 0 5 によってストリーム制御部 1 1 1 の指示により廃棄される。

【 0 0 6 . 6 】

図 1 4、図 1 5 は、出力ストリーム処理部 1 2 0 3 のクロスバススイッチの設定状態を示す図である。図 1 4 では、クロスバススイッチ 1 4 0 1 の接点 1 4 0 2、1 4 0 3 がオンに設定されている。

出力ストリーム処理部1203は、経路1221から入力される暗号化されたデータの番組情報を変更して出力インターフェース182に出力する。

【0067】

また、経路1231から入力される経路1211を経由した復号化されたデータを番組情報と、「スクランブルがかかっていない」のフラグとに変更して出力インターフェース181に出力する。

次に、出力ストリーム処理部1203に経路1231から入力される経路1213を経由した再暗号化されたデータが入力されたとき、ストリーム制御部111によって、図15に示すように、クロスバススイッチ1401の接点1403がオフにされ接点1501がオンにされる。これによって、再暗号化されたデータは、番組情報に変更され、出力インターフェース183に出力される。

【0068】

なお、経路1223から入力されるデータは、クロスバススイッチ1401の接点が全てオフ状態であるので、出力インターフェースに出力されることはない。

また、復号鍵131や暗号鍵133は、TV受信装置の制御部によって設定され、ストリーム制御部111に通知される。

本実施の形態において、外部のビデオ記録装置に出力する出力インターフェース183へのデータを再暗号化したのは、著作権を保護するためである。

【0069】

本実施の形態の動作は、本質的に実施の形態1のそれと異なるものではないので説明を省略する。

なお、上記各実施の形態において、鍵131～134は、入力インターフェース101～105から入力されるストリームデータに応じてTV受信装置の制御部において予め設定される。この鍵は、例えば、TV受信装置に挿入されたカードや受信されたストリームデータ中に記録されているものである。

【0070】

上記各実施の形態の構成図を図1、図6、図12に示したけれども、各構成要素の機能をコンピュータに発揮させるプログラムで実現するようにしてもよい。このプログラムをコンピュータ読み取り可能な記録媒体に記録して並列ストリー

ム暗復号装置に適用してもよいし、インターネット上のサイトに記録しておき、ダウンロードさせて並列ストリーム暗復号装置に適用してもよい。

【 0 0 7 1 】

【発明の効果】

以上説明したように、本発明は、ストリームデータを暗号化又は復号化する複数の鍵にそれぞれ対応する複数の経路と、入力される複数のストリームデータを、対応する経路に出力する入力ストリーム処理手段と、出力されたストリームデータを対応する鍵で暗号化又は復号化する暗復号演算手段とを備えることとしている。このような構成によって、暗復号演算手段は、ストリームデータの入力される経路に対応した鍵を用いて暗号化又は復号化することができるので、ストリームデータに応じていちいち鍵を選択する必要がなくなり、制御手順が簡略化される。

【 0 0 7 2 】

また、前記入力ストリーム処理手段は、クロスバスイッチを有し、ストリームデータの入力線とストリームデータを暗号化又は復号化する鍵に対応する経路に接続される出力線との接点のスイッチをオンに設定することにより、対応する経路にストリームデータを出力することとしている。このような構成によって、ストリームデータに対応した鍵の設定された経路に容易にストリームデータを出力することができる。

【 0 0 7 3 】

また、前記暗復号演算手段で暗号化又は復号化された複数のストリームデータの入力を受け、複数の出力インターフェースに各暗号化又は復号化されたストリームデータをそれぞれ出力する出力ストリーム処理手段を更に備えることとしている。このような構成によって、暗号化又は復号化されたストリームデータを適切な出力インターフェースに出力することができる。

【 0 0 7 4 】

また、前記出力ストリーム処理手段は、クロスバスイッチを有し、前記出力ストリーム処理手段から出力される複数の暗号化又は復号化されたストリームデータの出力先の出力インターフェースを前記経路に応じてクロスバスイッチをオン

オフ制御して切り換える制御手段と、複数の経路へ出力されたストリームデータと対応する鍵とを前記暗復号演算手段に経路毎に入力し、入力したストリームデータの経路情報を前記制御手段に通知する入力通知手段を更に備えることとしている。このような構成によって、ストリームデータを暗号化又は復号化したストリームデータの出力先の出力インターフェースを容易に設定することができる。

【 0 0 7 5 】

また、前記暗復号演算手段を複数備え、前記複数の経路へ出力されるストリームデータと対応する鍵とを各暗復号演算手段に並列入力し、各暗復号演算手段に入力したストリームデータの経路情報を通知する入力通知手段と、前記経路情報に従い、前記出力ストリーム処理手段から出力される複数の暗号化又は復号化されたストリームデータの出力先の出力インターフェースを選択制御する制御手段とを更に備えることとしている。このような構成によって、暗号化又は復号化を並列処理することができるので、暗号化又は復号化のスループットが向上する。

【 0 0 7 6 】

また、前記暗復号演算手段から出力された暗号化又は復号化されたストリームデータを再度前記入力ストリーム処理手段に入力する経路を更に備え、前記暗復号演算手段は、暗号化又は復号化されたストリームデータを異なる鍵で暗号化又は復号化することとしている。このような構成によって、例えば、暗号化又は復号化されたストリームデータを異なる暗号鍵によって再暗号化することができるので、著作権等の保護の実効を強化できる。

【 0 0 7 7 】

また、前記入力ストリーム処理手段は、入力される複数のストリームデータをマルチプレクス処理して1つのストリームデータを生成することとしている。このような構成によって並列して入力される複数のストリームデータから新たなストリームデータを生成した後、暗号化又は復号化をすることができる。

また、前記入力ストリーム処理手段は、入力される1つのストリームデータをデマルチプレクス処理して複数のストリームデータを生成することとしている。このような構成によって、例えば、複数の番組が多重化されたストリームデータの入力を受け、個々の番組のストリームデータに分離することができる。

【0078】

また、前記入力ストリーム処理手段は、入力される1つのストリームデータを2つの経路に出力し、1つの経路は、前記暗復号演算手段に、別の経路は、直接前記出力ストリーム処理手段にそれぞれ接続されていることとしている。このような構成によって、暗号化又は復号化を要しないストリームデータもいっしょに入力ストリーム処理手段に入力することができる。

【0079】

また、ストリームデータを暗号化又は復号化する複数の鍵にそれぞれ対応する複数の経路を備える並列ストリーム暗復号装置における並列ストリーム暗復号方法であって、入力される複数のストリームデータを、対応する経路に出力する入力ストリーム処理ステップと、出力されたストリームデータを対応する鍵で暗号化又は復号化する暗復号演算ステップとを有することとしている。このような方法によって、暗復号演算ステップにおいて、入力されるストリームデータに応じて鍵をいちいち選択する煩雑な操作の必要がなくなる。

【0080】

また、上記並列ストリーム暗復号方法をコンピュータに実行させるプログラムとしている。このようなプログラムをストリームデータを暗号化又は復号化する複数の鍵にそれぞれ対応する経路を有する並列ストリーム暗復号装置に適用して、暗号化又は復号化する鍵をいちいち選択する煩雑な操作を回避することができる。

【0081】

更に、上記並列ストリーム暗復号装置を組み込んだTV受信装置としている。このような構成によって、TV受信装置は、効率的に受信したストリームデータの暗号化又は復号化をすることが可能となる。

【図面の簡単な説明】

【図1】 本発明にかかる並列ストリーム暗復号装置の実施の形態1の構成図である。

【図2】 上記実施の形態の入力ストリーム処理部のクロスバスイッチのスイッチの状態を示す図である。

【図 3】 上記実施の形態の出力ストリーム処理部のクロスバスイッチのスイッチの状態の一例を示す図である。

【図 4】 上記実施の形態の出力ストリーム処理部のクロスバスイッチのスイッチの状態の他の例を示す図である。

【図 5】 上記実施の形態の動作を説明するフローチャートである。

【図 6】 本発明に係る並列ストリーム暗復号装置の実施の形態 2 の構成図である。

【図 7】 上記実施の形態の入力ストリーム処理部のクロスバスイッチの設定状態を示す図である。

【図 8】 上記実施の形態の出力ストリーム処理部のクロスバスイッチの設定状態を示す図である。

【図 9】 上記実施の形態の動作を説明するフローチャートである。

【図 10】 上記実施の形態の変形例の入力ストリーム処理部のクロスバスイッチの設定状態を示す図である。

【図 11】 上記各実施の形態の別の変形例の入力ストリーム処理部のクロスバスイッチの設定状態を示す図である。

【図 12】 本発明に係る並列ストリーム暗復号装置の実施の形態 3 の構成図である。

【図 13】 上記実施の形態の入力ストリーム処理部のクロスバスイッチの設定状態を示す図である。

【図 14】 上記実施の形態の出力ストリーム処理部のクロスバスイッチの設定状態を示す図である。

【図 15】 上記実施の形態の出力ストリーム処理部のクロスバスイッチの設定状態の他の例を示す図である。

【図 16】 従来の並列ストリーム暗復号装置の構成図である。

【符号の説明】

101～105	入力インターフェース
110	ストリーム解析部
111	ストリーム制御部

121, 1201 入力ストリーム処理部

131~134 鍵

141~144, 1211~1214, 1221~1224 経路

151 調停部

161 暗復号演算部

171, 607, 1203 出力ストリーム処理部

181~185 出カインターフェース

201, 301, 701, 801, 1001, 1101, 1301, 1401

クロスバススイッチ

601 第1暗復号演算部

602 第2暗復号演算部

603 第1調停部

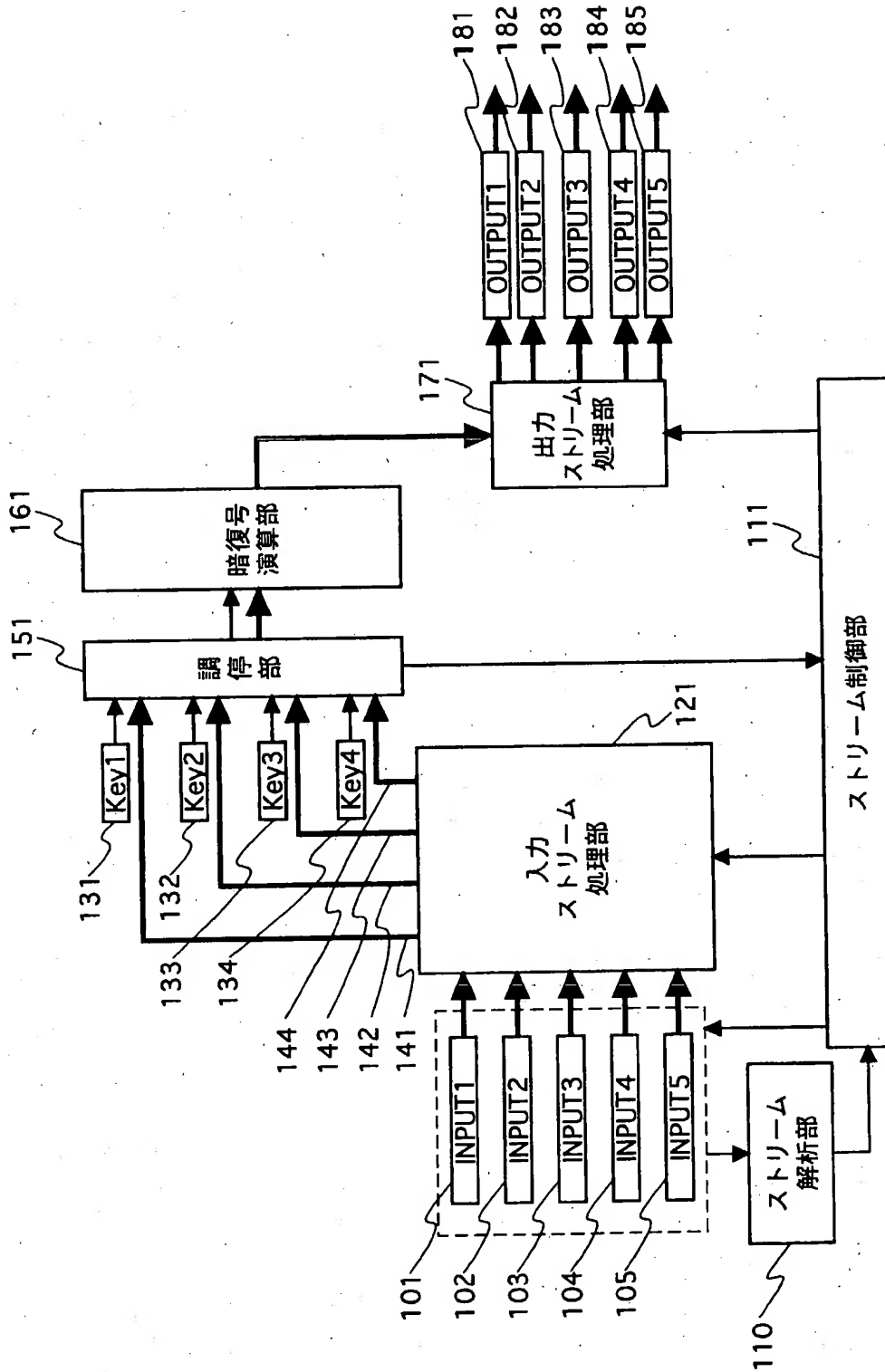
604 第2調停部

606, 607, 1231, 1241 経路

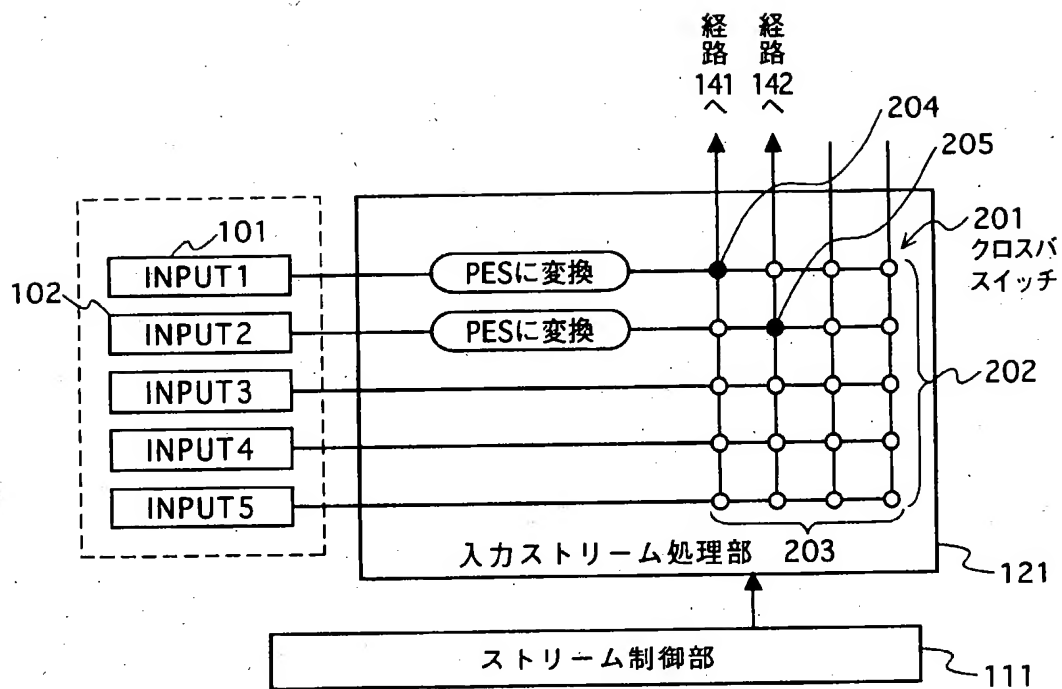
【書類名】

図面

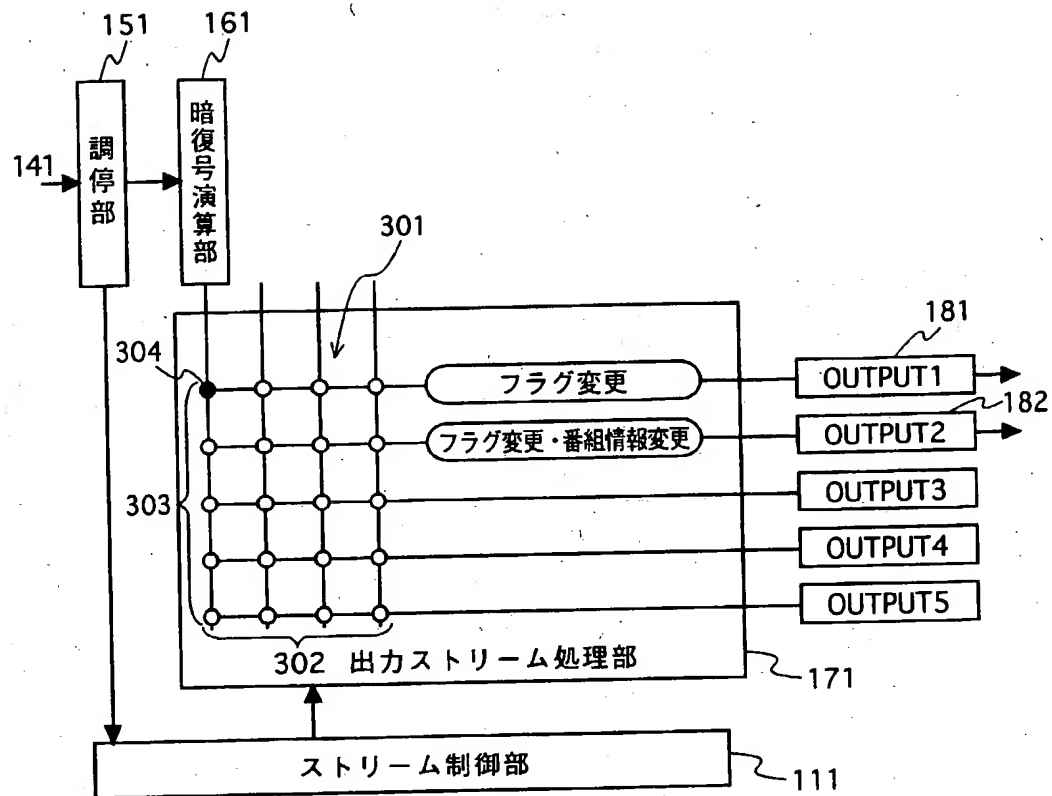
【図1】



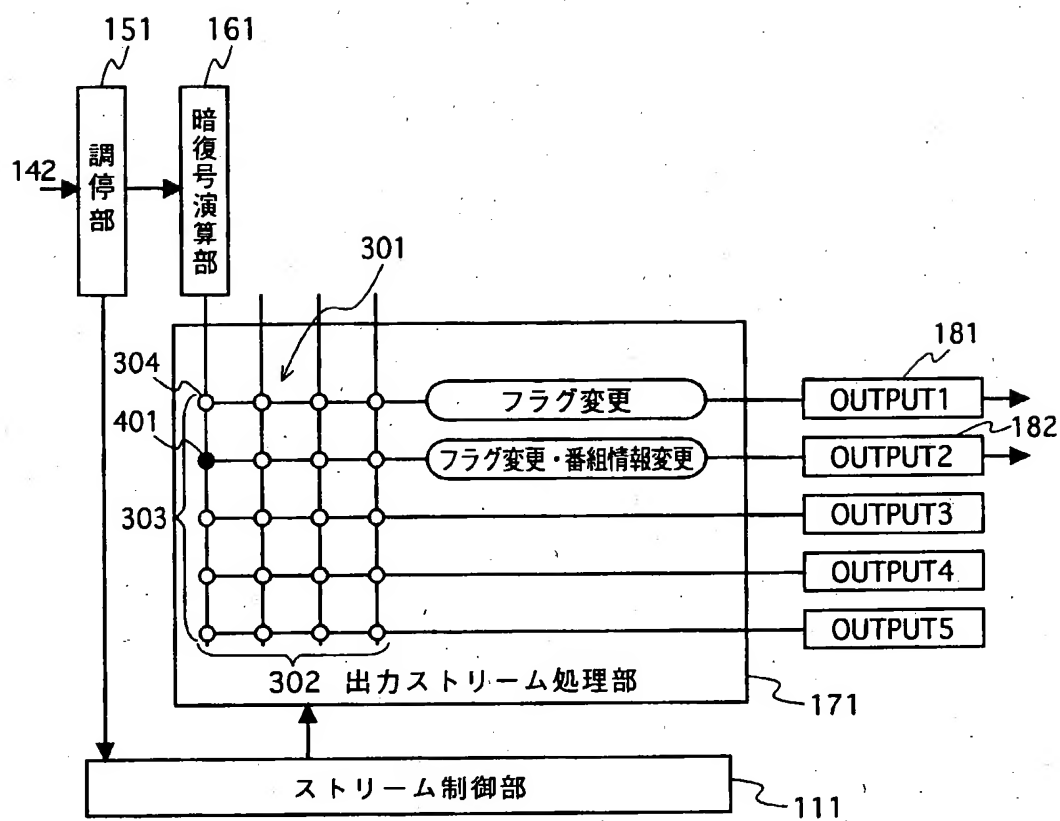
【図2】



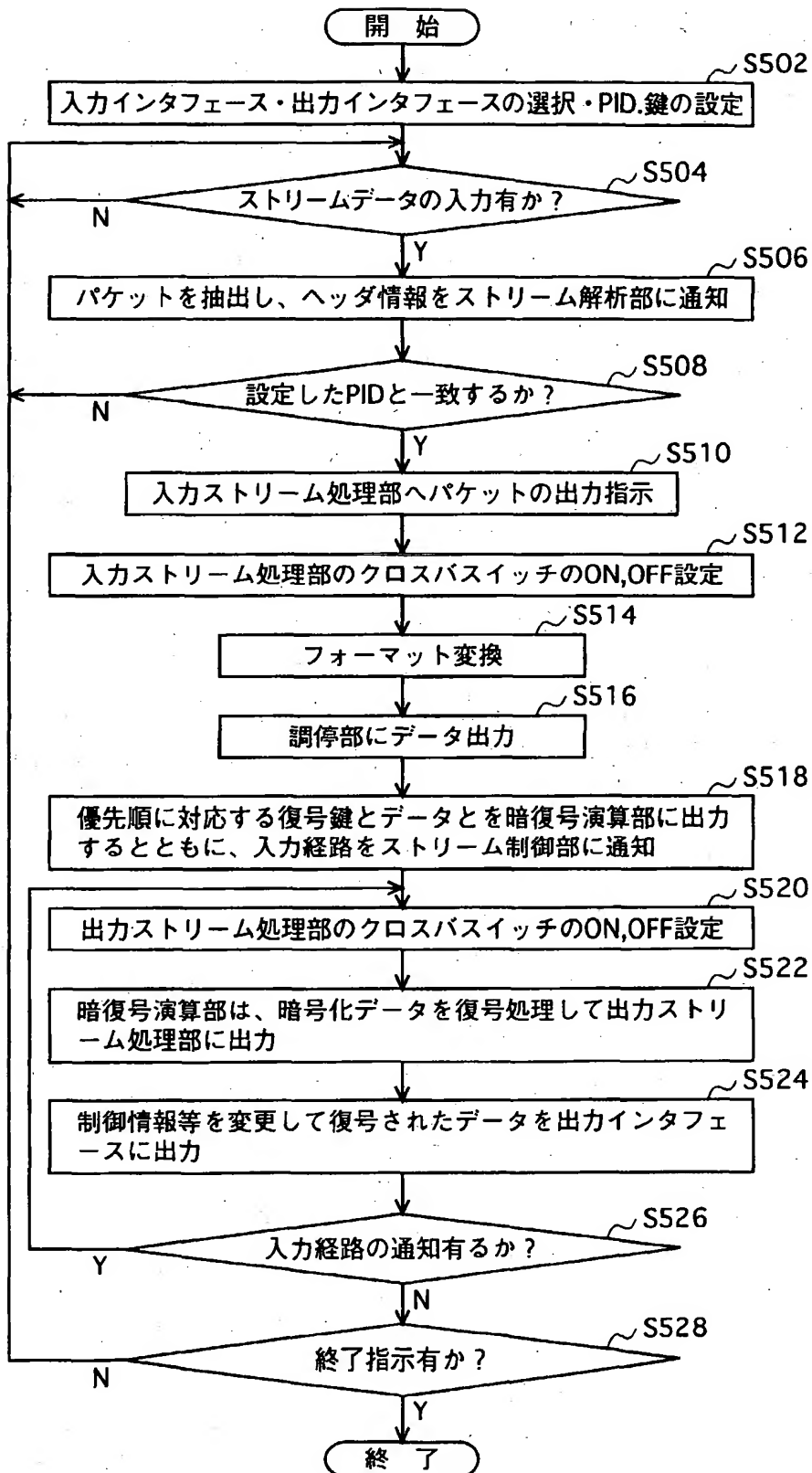
【図3】



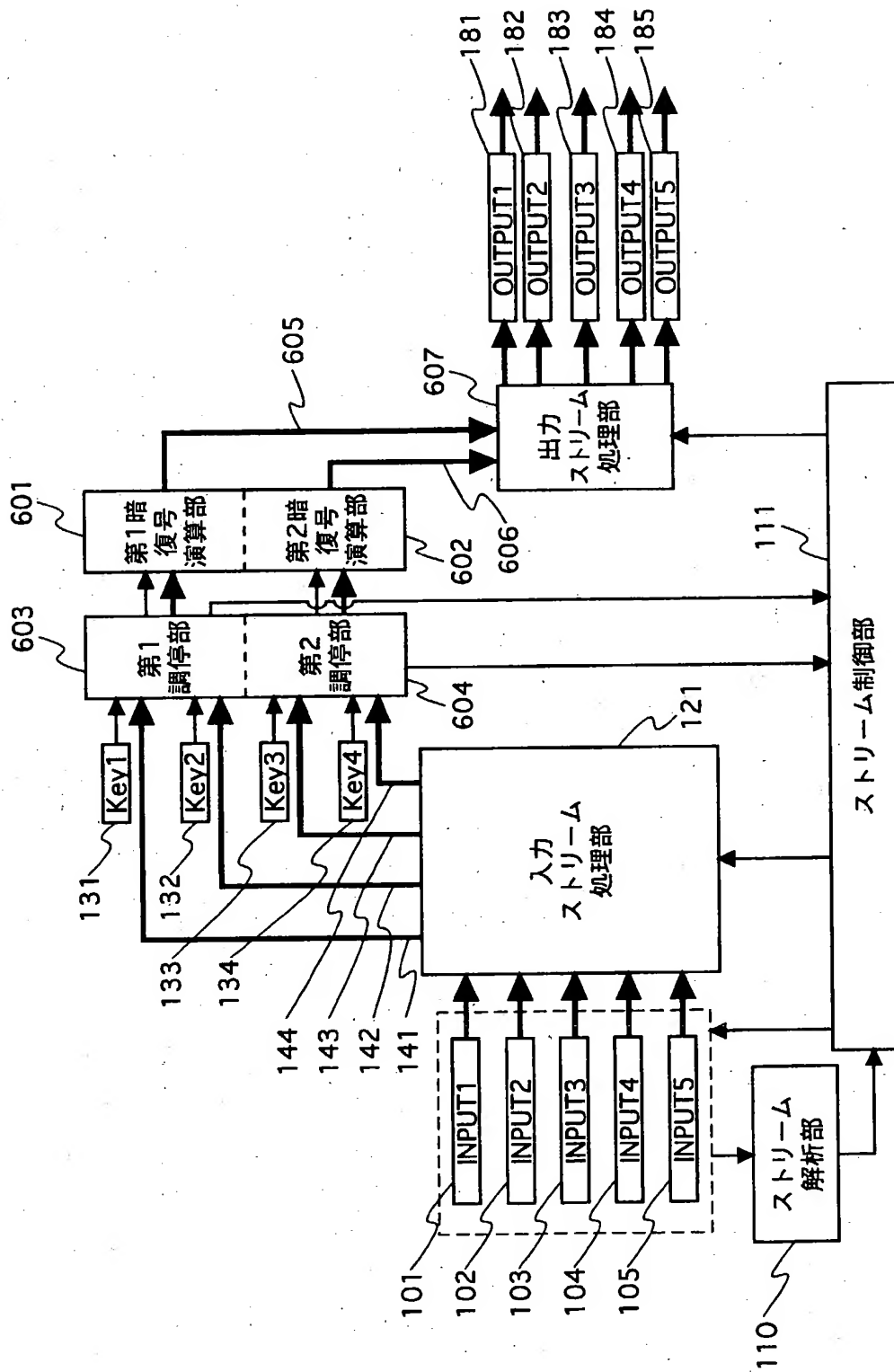
【図4】



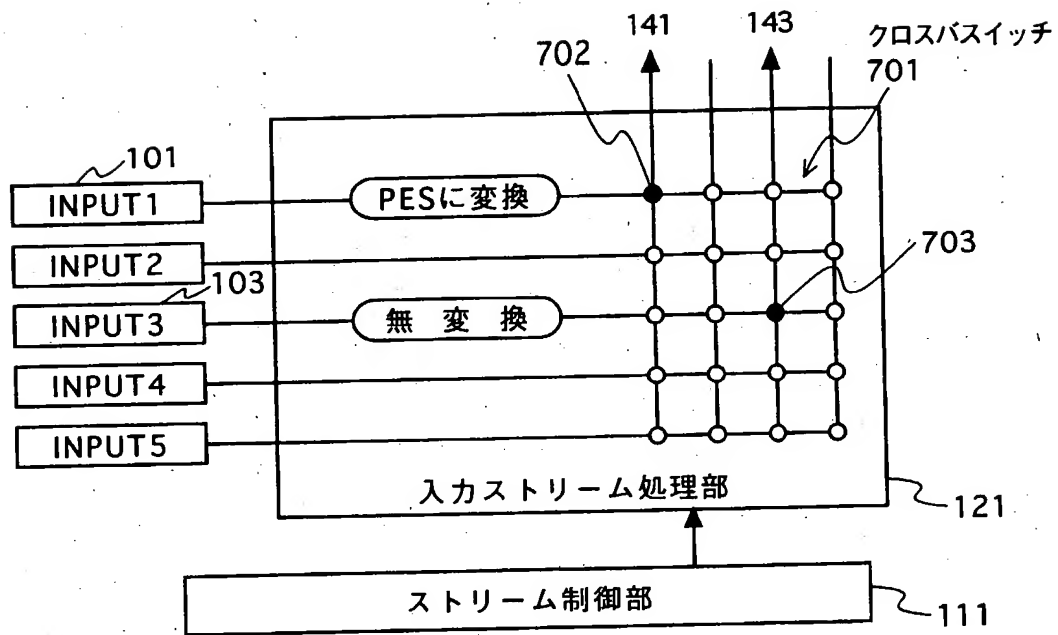
【図 5】



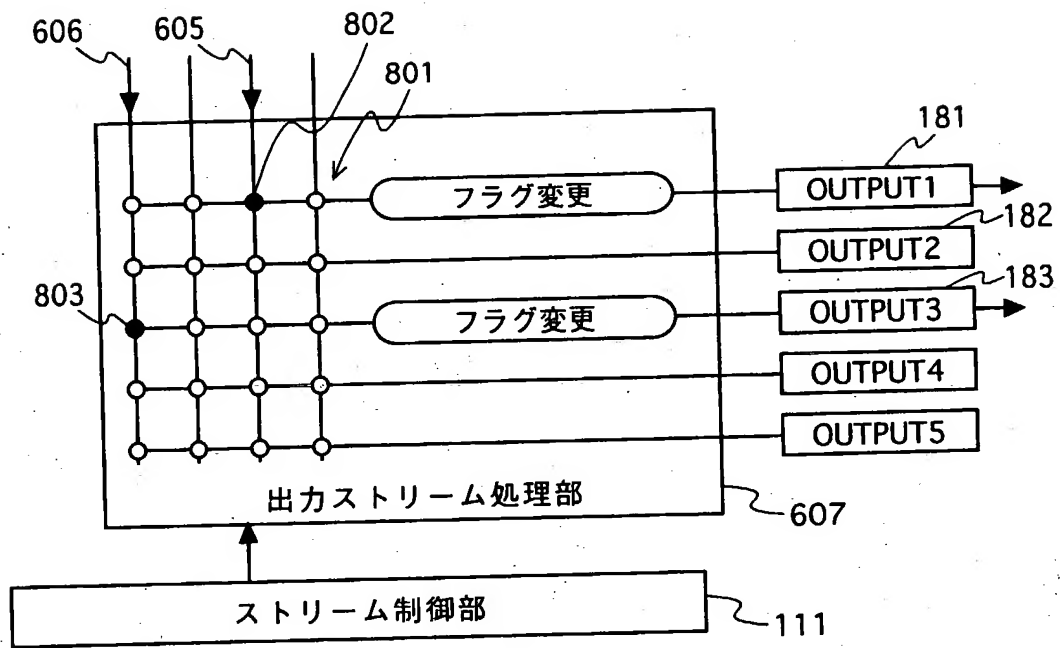
【図6】



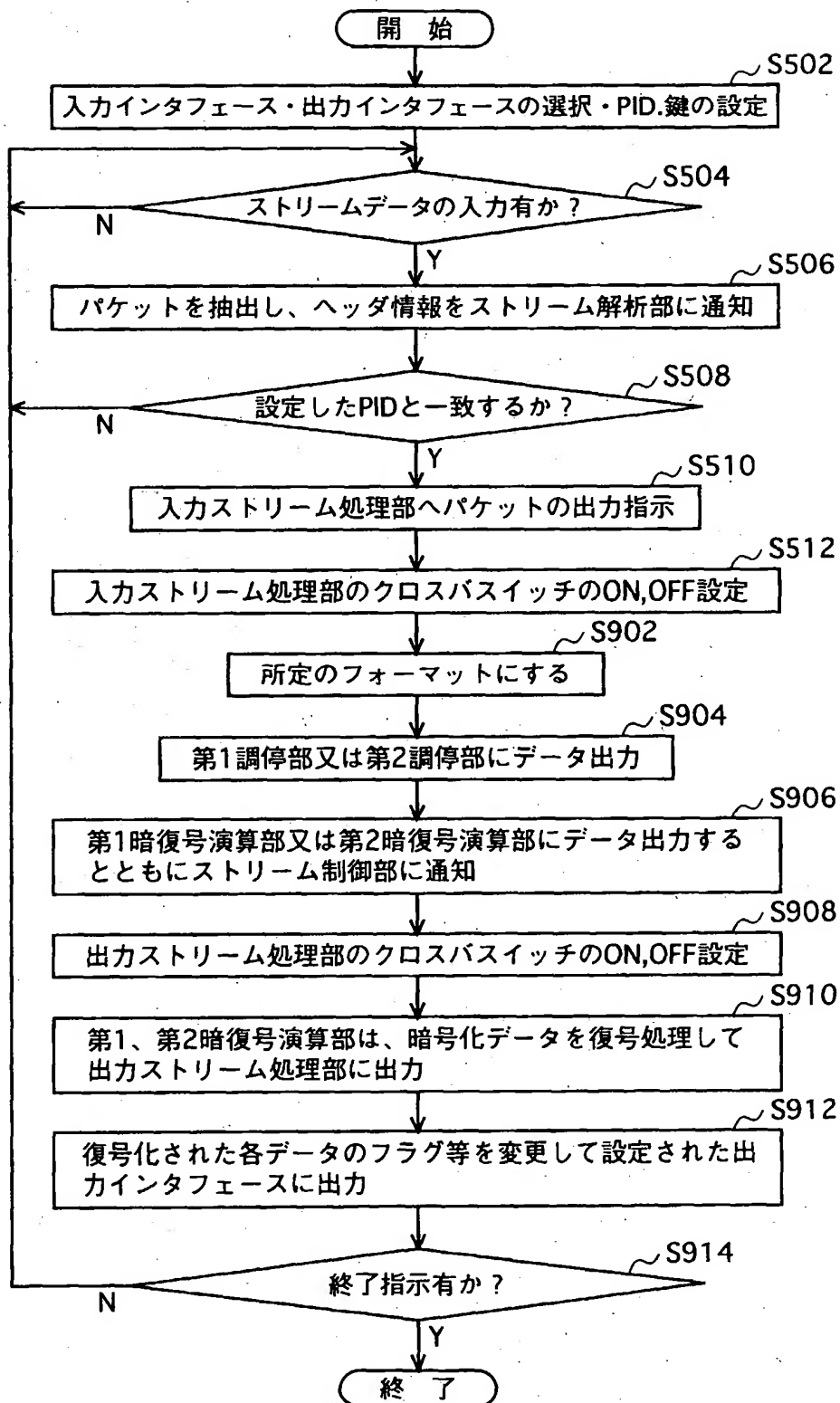
【図 7】



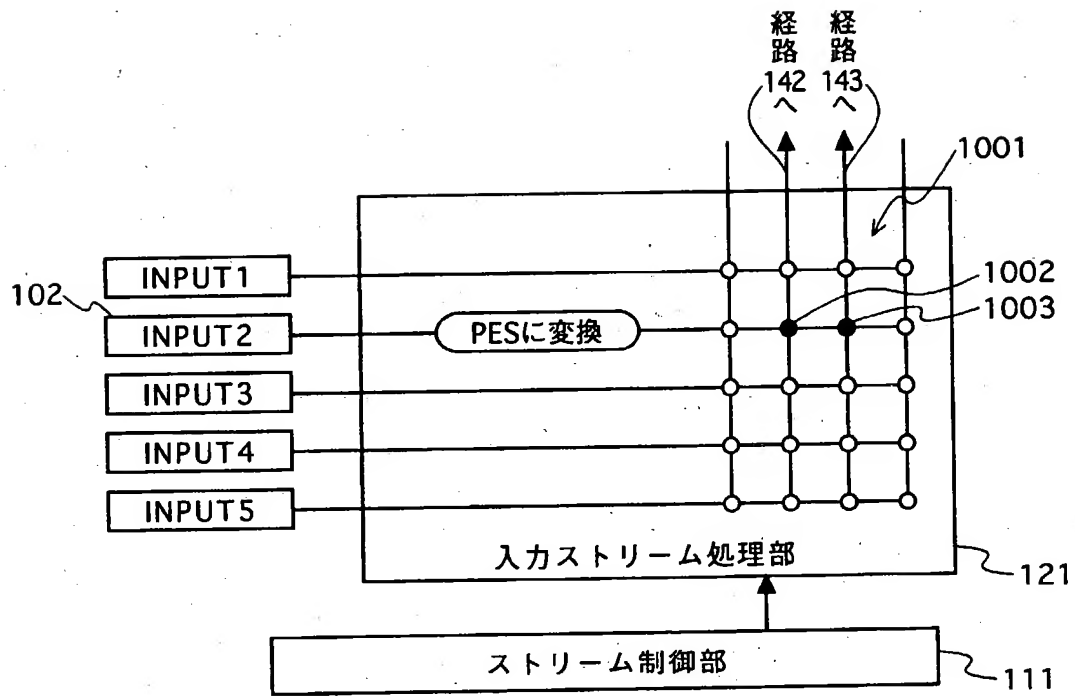
【図8】



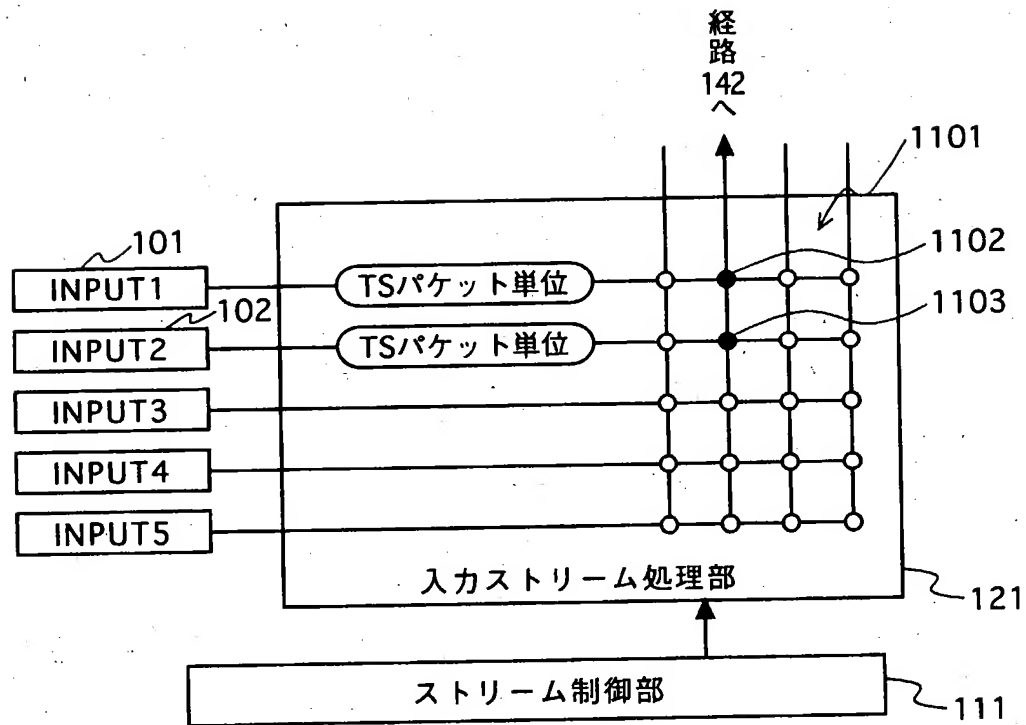
【図9】



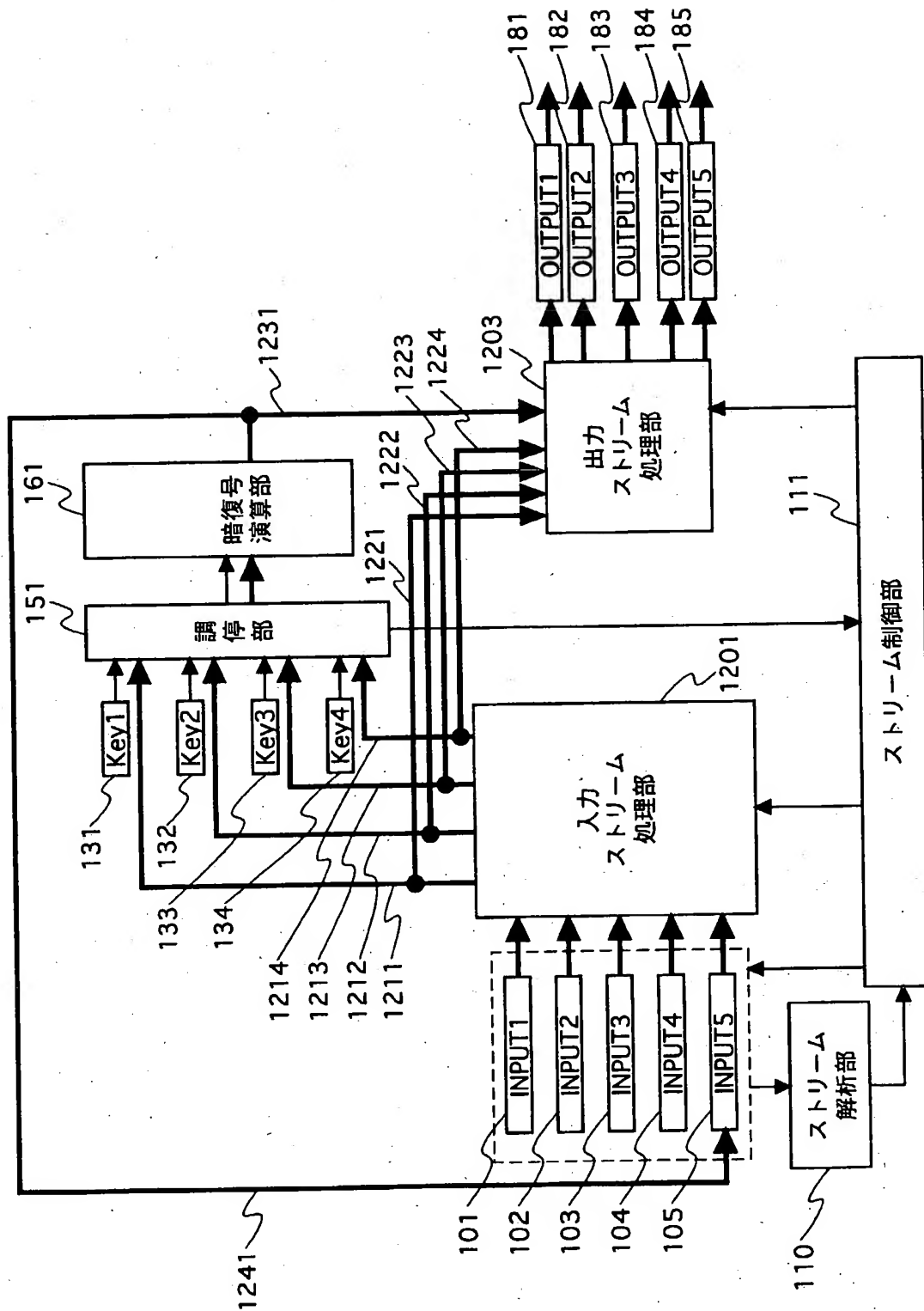
【図 1 0】



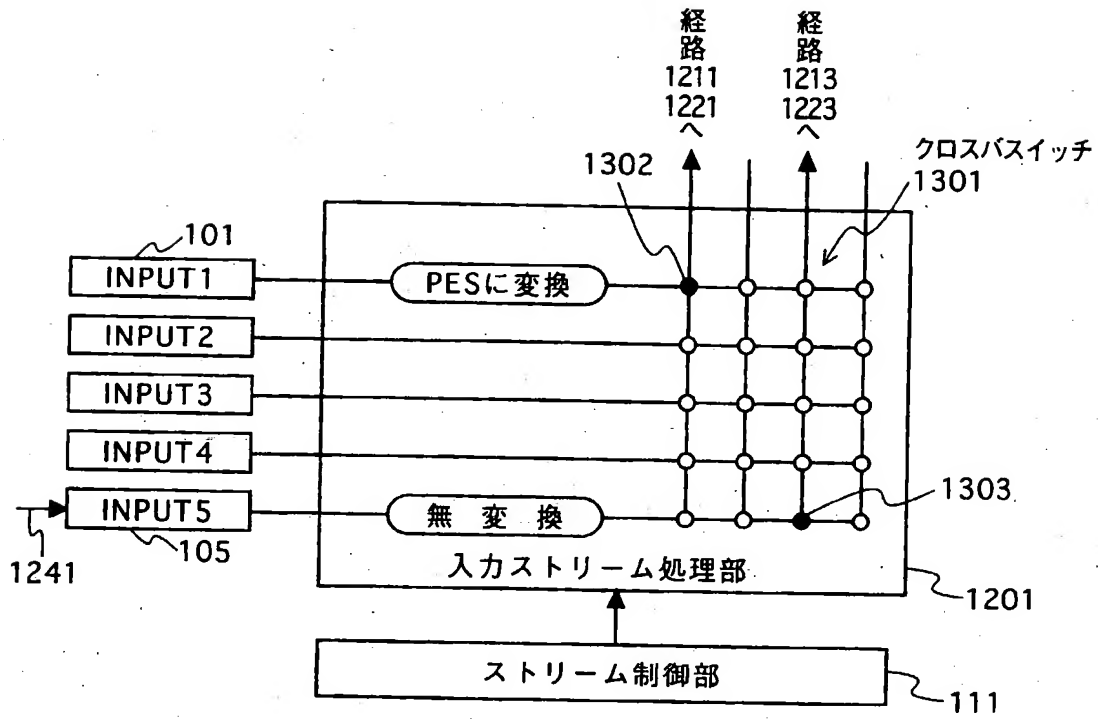
【図 1 1】



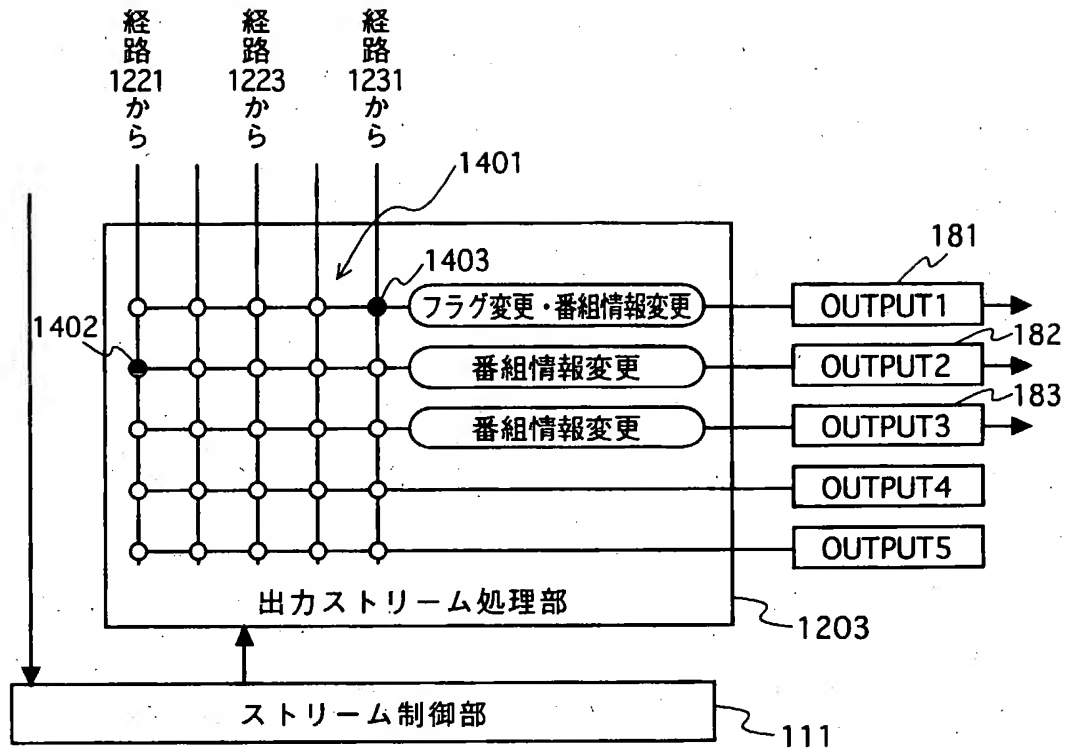
【図12】



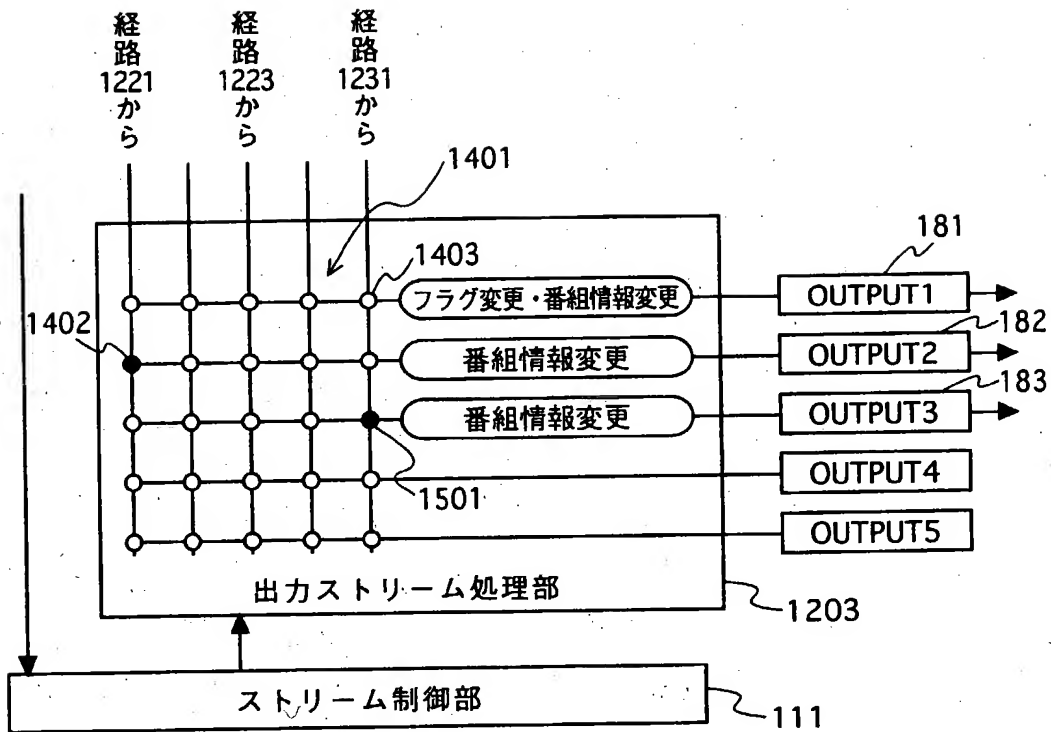
【図13】



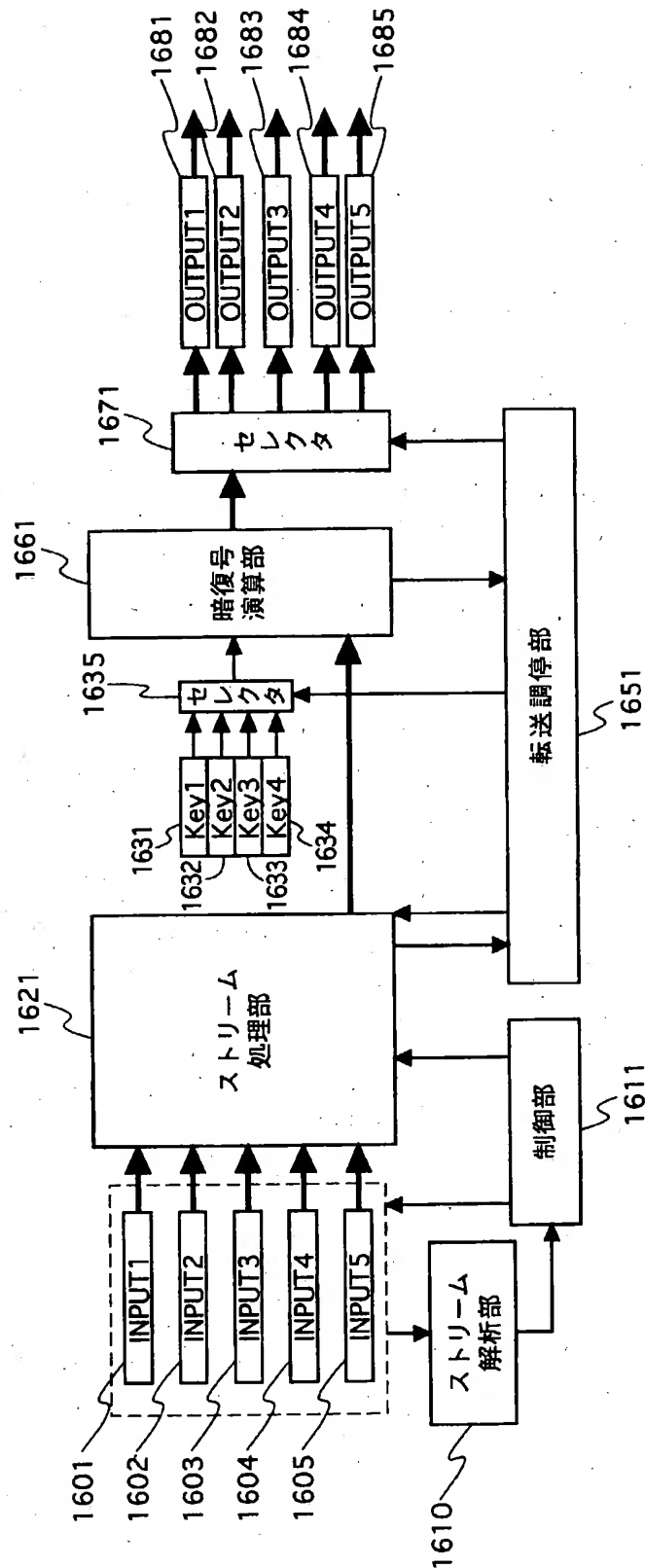
【図 1 4】



【図15】



【図16】



【書類名】 要約書

【要約】

【課題】 並列入力されるストリームデータを鍵を用いて暗号化又は復号化する並列ストリーム暗復号装置のストリームデータに対応する鍵の選択の煩雑さを回避する。

【解決手段】 ストリームデータを暗号化等する複数の鍵 1 3 1 ~ 1 3 4 に対応する経路 1 4 1 ~ 1 4 4 を設けている。入力インターフェース 1 0 1 から入力される T S は、復号鍵 1 3 1 で、入力インターフェース 1 0 2 から入力される T S は、復号鍵 1 3 2 で復号される。入力ストリーム処理部 1 2 1 は、入力インターフェース 1 0 1 から入力された T S データを復号鍵 1 3 1 に対応する経路 1 4 1 に、入力インターフェース 1 0 2 から入力された T S データを復号鍵 1 3 2 に対応する経路 1 4 2 に出力する。暗復号演算部 1 6 1 は、経路 1 4 1 から入力された T S データを復号鍵 1 3 1 で、経路 1 4 2 から入力された T S データを復号鍵 1 3 2 でそれぞれ復号する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社